



Safesign Identity Client para Mac OS X

Manual de Instalação e Configuração

As informações contidas neste manual estão sujeitas a alterações sem aviso prévio e não representam um compromisso por parte de PRONOVA CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA. Nenhuma parte deste manual poderá ser reproduzida de qualquer forma ou meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou sistemas de armazenamento e recuperação, sem o prévio consentimento, por escrito, de PRONOVA CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA.

Windows® é marca registrada da Microsoft Corporation

Pentium® é marca registrada da Intel Corporation

PRONOVA é marca registrada da Pronova Consultoria em Tecnologia da Informação Ltda.

PROTOKEN é marca registrada da Pronova Consultoria em Tecnologia da Informação Ltda.

SAFESIGN é marca registrada da A.E.T. Europe B.V.

Pronova Consultoria em Tecnologia da Informação Ltda.

Todos os produtos da Pronova Soluções Inteligentes (PRONOVA) incluindo, sem limitar-se a, cópias de avaliação, disquetes, CD-ROMs, hardware, software e documentação, e todos os futuros pedidos, estão sujeitos aos termos desta Licença. Se você não está de acordo com os termos aqui expostos, por favor, proceda a devolução do pacote completo e dentro do prazo de quinze dias úteis e reembolsaremos o custo do produto, exceto o frete e os encargos administrativos. Ao utilizar o produto você declara conhecer e aceitar os termos e condições do presente, que se formalizará em um contrato de Licença entre você e a PRONOVA, que também terá alcance aos distribuidores, revendas ou representantes da PRONOVA, com o alcance aqui convencionado.

1. **Uso Permitido** – Você pode fundir, relacionar e/ou fazer link do Software com outros programas com o único propósito de proteger esses programas de acordo com o uso descrito no Guia do Desenvolvedor que está junto com o produto, ou que pode ser encontrado no site web da PRONOVA (www.pronova.com.br). Você pode realizar cópias do Software com o fim de utilizá-las como cópias de segurança ou backup.

2. **Uso proibido** – O Software ou o hardware fornecido pela PRONOVA ou qualquer outra parte do Produto não pode ser reproduzida, copiada, reinventada, desmontada, descompilada, revisada, melhorada e modificada de qualquer forma, exceto como especificamente se permite no presente. Você não pode praticar engenharia reversa ao Software ou qualquer parte do produto, ou tentar descobrir o código fonte do Software. Você não pode usar o meio óptico ou magnético incluído com o produto com o propósito de transferir ou guardar dados que não fazem parte original de Produto, ou uma melhoria ou atualização de Produto fornecida pela PRONOVA.

3. **Garantia** – PRONOVA garante que os Produtos e os meios de armazenamento de Software são substancialmente livres de defeitos de fabricação ou materiais. Esta garantia terá validade por um período de tempo de 90 (noventa) dias desde a data de emissão da Nota Fiscal da PRONOVA.

4. **Fim da garantia** – No caso de que ocorra qualquer fato que produza o fim da garantia, a única obrigação por parte da PRONOVA é efetuar ou reparar a descrição da PRONOVA, qualquer produto sem que isto possa gerar algum encargo para você.

Para tanto PRONOVA ou revendas autorizadas, não serão responsáveis em nenhum caso por nenhum dano, prejuízo, gasto, ou conceito sobre a garantia expressamente reconhecida no presente. Em consequência a responsabilidade total faz de você ou qualquer terceiro por qualquer causa, tanto contratual como extracontratual, incluindo dolo, culpa ou negligência, não excederá, em nenhum caso, do preço que você pagou pelo Produto que tenha causado um dano, ou que tenha sido objeto de, ou indiretamente relacionado com, a causa do dano.

Em nenhum caso PRONOVA é responsável por nenhum dano causado por culpa ou negligência sua ou de terceiros, nem por nenhuma perda de dados, ganhos ou economias, ou por outros danos casuais ou casualidades, mesmo se PRONOVA tiver avisado da possibilidade de ocorrência ao dano. Qualquer produto que você entregará a PRONOVA com a finalidade de troca em comprimento desta garantia, passará a ser propriedade da PRONOVA.

5. **Limitação da Garantia** – A presente garantia não cobre e nem cobrirá defeitos provocados por uso inadequado ou conservação do produto. A garantia também se perderá se for verificado que o produto foi, de qualquer modo, aberto, forçado, desarmado ou que tenha sido feito qualquer um dos Usos Proibidos detalhados no presente.

Para invocar a garantia, é necessário se comunicar por escrito com a PRONOVA, durante o período de garantia, previsto da presente garantia e a nota fiscal de compra do produto. PRONOVA terá direito de avaliar o produto em até 15 dias, ou por um prazo maior desde que o defeito seja importante. Qualquer produto que você devolver a PRONOVA deverá ser enviado com frete e seguro pré-pago.

Exceto as condições expostas, PRONOVA não outorga outra garantia dos produtos do que as expressamente detalhadas no presente. Para tanto não poderá se estender que exista extensão ou maior alcance da mesma, tanto expressa com implícita, incluindo, podem sem limitar-se a possibilidade do uso do produto para um propósito em particular.

6. **Término da Garantia** – Esta licença será considerada automaticamente terminada em qualquer caso em que você não cumprir total ou parcialmente os termos deste contrato.

Índice

Política de Garantia Pronova	5
1. Glossário	11
2. Lista de Acrônimos	15
3. Sobre a Pronova Soluções Inteligentes	17
4. Introdução	17
5. Pré-requisitos	17
6. Ambientes Homologados	17
7. Hardwares Homologados	18
8. Instruções de Instalação	18
8.2 Como iniciar a instalação?	19
8.3 – Como verificar a instalação?	24
8.4 – Como visualizar o meu certificado?	26
8.5 – Como testar o meu certificado usando o Mozilla Firefox?	26
9. Perguntas e Respostas	32
10. Suporte Técnico	33

Política de Garantia Pronova

IMPORTANTE-LEIA ESTA GARANTIA DO FABRICANTE COM ATENÇÃO PARA ENTENDER SEUS DIREITOS E OBRIGAÇÕES! O termo "Dispositivo de Hardware" significa o produto de hardware Pronova. O termo "Você" significa uma pessoa física ou jurídica que será referida nesta Garantia Limitada como "Você" e "Seu(s)/Sua(s)".

A. GARANTIAS.

1. Garantia Expressa. *Você* estará sujeito aos termos e condições desta Garantia Limitada e, em substituição a quaisquer outras (se houver) garantias expressas, a Pronova garante a *Você*, sob condições normais de uso e serviço, na data da aquisição identificada no recibo ou no comprovante de pagamento e pelo período de tempo especificado abaixo para o Dispositivo de Hardware aplicável (doravante denominados o "Prazo de Garantia"), que o Dispositivo de Hardware será executado substancialmente em conformidade com o descrito na embalagem e na documentação da Pronova que o acompanha. Relativamente ao descobrimento de defeitos após o Prazo de Garantia, a Pronova não fornecerá qualquer tipo de garantia ou condição.

A PRONOVA assegura total cobertura contra defeito de fabricação para os produtos fornecidos ao cliente no território brasileiro, durante o período da garantia.

Prazo de Garantia

Garantia Legal - 90 (noventa) dias

A garantia legal praticada pela PRONOVA obedece aos dispositivos relacionados no artigo 26 do Código de Defesa do Consumidor (CDC), e é direito do consumidor que apresente a reclamação comprovadamente formulada no prazo de 90 (noventa) dias da data de aquisição do produto PRONOVA para troca do produto e/ou serviço adquirido por igual ou equivalente superior.

A reposição dos produtos em garantia estará sujeita às condições de retorno do produto, observando a garantia legal, conforme art. 50 do CDC.

PRAZO TOTAL DA GARANTIA:

- (I) Para todos os conjuntos de Tokens USB: 90 (noventa) dias;
- (II) Leitor de cartão inteligente: 90 (noventa) dias;
- (III) Cartão Inteligente: 90 (noventa) dias.

CONCORDANDO COM A GARANTIA CONTRATUAL, O CONSUMIDOR ABRE MÃO DE QUAISQUER RECLAMAÇÕES APÓS O PERÍODO DE 90 (noventa) DIAS, TEMPO CONSIDERADO SUFICIENTE PARA A IDENTIFICAÇÃO DE QUAISQUER PROBLEMAS NO PRODUTO OU NA PRESTAÇÃO DE SERVIÇOS.

Os dispositivos criptográficos (tokens e cartões) e leitores de cartão inteligente vendidos pela PRONOVA têm garantia contra defeitos de fabricação pelo prazo de 90 (noventa) dias contados a partir da data de aquisição do produto PRONOVA.

Os dispositivos criptográficos (tokens e cartões) armazenam o seu Certificado Digital protegendo-o contra acessos indevidos. AS SENHAS (PIN, PUK, SENHA, FRASE SENHA OU PASSWORD) PARA ACESSO A ESSES DISPOSITIVOS SÃO SOMENTE DE CONHECIMENTO E RESPONSABILIDADE DO TITULAR OU RESPONSÁVEL DO CERTIFICADO DIGITAL, E A PRONOVA NÃO MANTÉM CÓPIAS OU POSSUI MEIOS DE RECUPERÁ-LAS.

CASO O DISPOSITIVO CRIPTOGRÁFICO SEJA BLOQUEADO OU INUTILIZADO DEVIDO À PERDA DAS SENHAS, SEU CONTEÚDO SERÁ PERDIDO. A REPOSIÇÃO DESTES DISPOSITIVOS (E DE SEU CONTEÚDO) NÃO É COBERTA PELA POLÍTICA DE GARANTIA PRONOVA.

Caso o Serviço de Suporte Técnico PRONOVA constate defeito de fabricação que requeira a substituição do dispositivo criptográfico durante o período de vigência desta garantia, a PRONOVA:

- Efetuará troca do dispositivo criptográfico, sem custo adicional para o cliente; e
- Não emitirá um novo certificado, sem custo adicional para o cliente, caso o defeito de fabricação acarrete na perda do Certificado Digital.

Essa Garantia Limitada não cobrirá, bem como não será fornecido qualquer tipo de garantia para aspectos subjetivos ou estéticos do Dispositivo de Hardware. A garantia expressa prevista acima constitui a única garantia expressa concedida a Você e é fornecida em substituição a todas as outras condições e garantias, sejam

expressas ou implícitas (exceto quaisquer garantias implícitas existentes que não possam ser recusadas), inclusive aquelas criadas por qualquer outra documentação ou embalagem. Qualquer informação ou sugestão (oral ou escrita) fornecida pela Pronova, por seus agentes, afiliadas ou subsidiárias ou por seus funcionários ou agentes, não criará qualquer garantia ou condição ou ampliará o escopo desta Garantia Limitada.

2. Limitação da Vigência das Garantias Implícitas. Se Você for um consumidor estrangeiro, também poderá ter uma condição e/ou garantia implícita de acordo com a legislação de algumas jurisdições, a qual é limitada pela vigência do presente Prazo de Garantia.

B. RECURSO EXCLUSIVO. Sujeito à legislação aplicável e às disposições a seguir, e desde que Você, durante o Prazo de Garantia, devolva o Dispositivo de Hardware à Pronova, com uma cópia do recibo ou comprovante válido de pagamento, a Pronova irá, a seu critério:

(i) reparar ou substituir o Dispositivo de Hardware; ou (ii) indenizá-lo pelos danos diretos sofridos por Você, limitando-se a responsabilidade ao valor efetivamente pago por Você pelo Dispositivo de Hardware.

(ii) Qualquer Dispositivo de Hardware reparado ou substituído conforme esta Garantia Limitada terá garantia pelo Prazo de Garantia original remanescente ou por 30 (trinta) dias, a partir da data de devolução do item para Você, o que for maior.

Salvo previsão expressa em contrário pela legislação aplicável, Você deverá arcar com os custos relacionados ao transporte (inclusive embalagem) do produto dentro do prazo da garantia; e

C. ISENÇÃO DE OUTRAS GARANTIAS. A garantia expressa especificada acima é a única garantia expressa oferecida a Você e é fornecida em substituição a todas as outras condições e garantias expressas ou implícitas (se houver), inclusive aquelas criadas por qualquer outra documentação ou embalagem. Nenhuma outra garantia é fornecida em relação ao Dispositivo de Hardware ou aos serviços de garantia por qualquer pessoa, incluindo, mas não se limitando a, a Pronova, os seus agentes, as afiliadas e os fornecedores. Nenhuma informação ou sugestão (oral ou escrita) fornecida pela Pronova, por seus agentes, afiliadas ou subsidiárias ou por seus funcionários ou agentes, deverá criar uma garantia ou condição ou ampliar o escopo

desta Garantia Limitada. Também não há garantias ou condições de titularidade, uso pacífico ou não-violação de direitos de autor no Dispositivo de Hardware.

D. EXCLUSÃO DE OUTROS DANOS.

NA EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL, A PRONOVA, SEUS AGENTES, AFILIADAS E/OU FORNECEDORES NÃO SERÃO RESPONSÁVEIS POR QUALQUER:

(i) DANO CONSEQÜENCIAL OU INCIDENTAL;

(ii) DANOS POR LUCROS CESSANTES, INTERRUPÇÃO DE NEGÓCIOS, PERDA DE DADOS, INFORMAÇÕES CONFIDENCIAIS OU OUTRAS, PERDA DE PRIVACIDADE, QUALQUER INABILIDADE NO USO DO DISPOSITIVO DE HARDWARE, NO TODO OU EM PARTE, DANOS PESSOAIS OU QUALQUER FALHA NO CUMPRIMENTO DE QUALQUER OBRIGAÇÃO (INCLUINDO MAS NÃO SE LIMITANDO A QUALQUER OBRIGAÇÃO GERADA EM RELAÇÃO A CASO DE NEGLIGÊNCIA E QUEBRA DO PRINCÍPIOS DE BOA-FÉ E DO ESFORÇO DE APRIMORAMENTO);

(iii) DANO INDIRETO, ESPECIAL OU PUNITIVO DECORRENTE DO OU DE QUALQUER FORMA RELACIONADO COM O DISPOSITIVO DE HARDWARE.

(iii) QUALQUER TIPO DE INFORMAÇÃO QUE VENHA A SER ARMAZENADA NOS EQUIPAMENTOS COMERCIALIZADOS PELA PRONOVA.

AS EXCLUSÕES ACIMA SERÃO APLICADAS MESMO QUE A PRONOVA OU QUALQUER AGENTE, AFILIADA OU FORNECEDOR TENHA SIDO ALERTADO SOBRE A POSSIBILIDADE DE OCORRÊNCIA DE TAIS PERDAS OU DANOS, E MESMO QUE HAJA FALHA, DANO (INCLUSIVE NEGLIGÊNCIA), RESPONSABILIDADE OBJETIVA OU PELO FATO DO PRODUTO, DECLARAÇÃO FALSA OU QUALQUER OUTRO MOTIVO.

E. EXCLUSÕES DE COBERTURA. A Garantia Limitada não será aplicável e a Pronova, seus agentes, afiliadas e/ou fornecedores não terão qualquer responsabilidade relativa a esta Garantia Limitada se o Dispositivo de Hardware:

(i) for usado para fins comerciais (inclusive aluguel ou arrendamento);

(ii) for modificado ou adulterado;

(iii) for danificado por motivos de força maior, alta-tensão, uso indevido, abuso,

negligência, acidente, desgaste, manipulação indevida, aplicação errada ou outras causas não relacionadas a defeitos no Dispositivo de Hardware;

(iv) for danificado por programas, informações, vírus ou arquivos ou durante envios ou transmissões;

(v) não for usado de acordo com a documentação e as instruções de uso que o acompanham; ou

(vi) for reparado, modificado ou alterado por outra pessoa que não seja um representante da assistência técnica autorizada da Pronova e se a assistência técnica não autorizada causar ou contribuir para o surgimento de qualquer defeito ou dano.

F. REGISTRO. Não é necessário registrar a aquisição do Dispositivo de Hardware para que essa Garantia Limitada tenha validade.

G. BENEFICIÁRIO. Na extensão máxima permitida pela lei aplicável, a Garantia Limitada será concedida exclusivamente a Você, o primeiro adquirente do Dispositivo de Hardware, não existindo outros beneficiários da Garantia Limitada. Salvo previsão expressa em contrário na lei, esta Garantia limitada não será destinada, bem como não será aplicável a qualquer outra pessoa, inclusive qualquer pessoa para a qual Você faça uma transferência do Dispositivo de Hardware.

H. INFORMAÇÕES ADICIONAIS. A Pronova é a entidade que fornece esta Garantia Limitada. Para receber instruções sobre como executar esta Garantia Limitada, entre em contato com uma subsidiária Pronova de sua localidade ou escreva para; Pronova Soluções Inteligente, Avenida das Américas 500, bloco 4, sala 302, Barra da Tijuca, Rio de Janeiro, RJ, CEP 22.640-100, ou visite a Pronova na Internet no endereço <http://www.pronova.com.br>

Outras exigências:

1. Você deverá enviar um comprovante de pagamento na forma de uma fatura (ou uma cópia) ou um recibo autêntico com data evidenciando que Você é o beneficiário desta Garantia Limitada e que a Sua solicitação está sendo feita dentro do Prazo de Garantia.

2. Para execução da Garantia Limitada, Você deverá levar ou enviar o item na sua embalagem original ao local especificado pela Pronova. Salvo previsão expressa em

contrário prevista na legislação aplicável, Você arcará com os custos relacionados ao transporte (inclusive embalagem) do serviço dentro do prazo da garantia.

Caso não siga as instruções acima, Você poderá ter despesas adicionais, poderá perder a sua garantia ou poderão ocorrer atrasos.

As informações contidas neste documento, incluindo URLs e outras referências a sites na Internet, estão sujeitas a alterações sem aviso prévio. Salvo indicação em contrário, os exemplos de empresas, organizações, produtos, nomes de domínio, endereços de e-mail, logotipos, pessoas, lugares e acontecimentos aqui mencionados são fictícios e nenhuma associação com qualquer empresa, organização, produto, nome de domínio, endereço de e-mail, logotipo, pessoa ou acontecimento real é intencional ou deve ser inferida.

Obedecer a todas as leis de direitos autorais aplicáveis é responsabilidade do usuário. Sem limitar os direitos autorais, nenhuma parte deste documento pode ser reproduzida, armazenada ou introduzida em um sistema de recuperação, ou transmitida de qualquer forma por qualquer meio (eletrônico, mecânico, fotocópia, gravação ou qualquer outro), ou para qualquer propósito, sem a permissão expressa e por escrito da Pronova.

A Pronova pode ter patentes ou requisições para obtenção de patente, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual que abrangem o conteúdo deste documento. A posse deste documento não lhe confere nenhum direito sobre as citadas patentes, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual, salvo aqueles expressamente mencionados em um contrato de licença, por escrito, da Pronova.

© 2004-2013 Pronova Soluções Inteligentes. Todos os direitos reservados.

Pronova é marca registrada ou comercial da Pronova Consultoria em Tecnologia da Informação Ltda. na República Federativa do Brasil e/ou em outros países.

Os nomes de produtos e de empresas reais aqui mencionados podem ser marcas comerciais de seus respectivos proprietários.

A Pronova concede ao comprador deste produto o direito de reproduzir uma (1) cópia do "Manual de Instruções" impresso para cada Dispositivo de Hardware adquirido na embalagem.

1. Glossário

Assinatura Digital: Resultado de uma transformação criptográfica de dados, que quando implementada apropriadamente, provê os seguintes serviços de segurança: autenticação da origem, integridade de dados e não repúdio do signatário;

Atribuição de chaves (key establishment): Processo que possibilita atribuir uma chave simétrica para uso criptográfico aos participantes legítimos de uma sessão de comunicação. A atribuição de chaves pode ser realizada por meio de duas técnicas: “Negociação de Chaves” ou “Transferência de Chaves”;

Autoridade Certificadora (AC): Entidade idônea autorizada a emitir, renovar e cancelar certificados digitais. É responsável pela administração das chaves públicas;

Autoridade de Registro (AR): É uma entidade operacionalmente vinculada à determinada Autoridade Certificadora Habilitada, responsáveis pela confirmação da identidade dos solicitantes dos certificados e-CPF e e-CNPJ;

Certificado Digital: Documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular. A função precípua do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública;

Chave criptográfica: Código ou parâmetro usado em conjunto com um algoritmo criptográfico, determinando as seguintes operações:

- Transformação de dados em texto claro para um formato cifrado e vice-versa;
- Assinatura digital computada a partir de dados;
- Verificação de uma assinatura digital computada a partir de dados;
- Geração de um código de autenticação computado a partir de dados; ou
- Um acordo para troca de um segredo compartilhado;

Chave Criptográfica em texto claro: representa uma chave criptográfica não cifrada;

Chave secreta: Chave criptográfica, usada com um algoritmo criptográfico de chave secreta, que está unicamente associada a uma ou mais entidades e não deveria tornar-se pública;

Código de Autenticação: corresponde a um verificador de integridade criptográfico que é comumente referenciado como MAC (Message Authentication Code);

Co-assinatura: A co-assinatura (ou sign) é aquela gerada independente das outras assinaturas;

Contra-assinatura: A contra-assinatura (ou countersign) é aquela realizada sobre uma assinatura já existente. Na especificação PKCS#7, a contra-assinatura é adicionada na forma de um atributo não autenticado (countersignature attribute) no bloco de informações (signerInfo) relacionado a assinatura já existente;

Elemento de Dado: Corresponde a um item de informação para o qual são definidos um nome, uma descrição de conteúdo lógico, um formato e uma codificação [ISO/IEC 7816-4];

Entidade usuária externa: Um indivíduo ou processo que realiza acesso a um módulo criptográfico independentemente do papel assumido;

FIPS (Federal Information Processing Standards): correspondem a padrões e diretrizes desenvolvidos e publicados pelo NIST (National Institute of Standards and Technology) para uso de sistemas computacionais no âmbito governamental federal norte-americano. O NIST desenvolve os padrões e diretrizes FIPS, quando há requisitos obrigatórios do governo federal, tais como, segurança e interoperabilidade, e não há padrões ou soluções industriais aceitáveis;

Firmware: Programas e componentes de dados de um módulo que estão armazenados em hardware (ROM, PROM, EPROM, EEPROM ou FLASH, por exemplo) e não podem ser dinamicamente escritos ou modificados durante a execução;

Fronteira criptográfica (cryptographic boundary): A fronteira criptográfica é um perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico.

Hardware: Parte ou equipamento físico usado para processar programas e dados;

ICP-Brasil: conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras;

Identificador de Registro: Valor associado a um registro que pode ser usado para referenciar aquele registro. Diversos registros poderiam ter o mesmo identificador dentro de um EF [ISO/IEC 7816-4];

Integridade: propriedade que determina que dados não devem ser modificados ou apagados de uma maneira não autorizada e indetectável;

Interface: representa um ponto lógico de entrada e saída de dados, que provê acesso aos serviços disponíveis pelos módulos criptográficos;

Interface CryptoAPI: Interface de operação de criptografia desenvolvida pela Microsoft. Esta interface oferece ao dispositivo independência ou implementação de encapsulamento de algoritmos criptográficos, permitindo aos desenvolvedores uma fácil utilização destes algoritmos em suas aplicações PKI, incluindo criptografia de dados, verificação de certificados e assinatura digital na plataforma Windows;

ITI: autarquia federal vinculada à Casa Civil da Presidência da República. O ITI é a Autoridade Certificadora Raiz - **AC Raiz** da Infraestrutura de Chaves Públicas Brasileira - **ICP-Brasil**. Como tal é a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

Middleware: Software que é usado amarrar uma aplicação;

Módulo criptográfico (cryptographic module): Conjunto de hardware, software e/ou firmware que implementa funções ou processos criptográficos, abrangendo algoritmos criptográficos e de geração de chaves;

Módulo criptográfico de chip único (Single-chip Cryptographic Module): representa uma materialização física na qual um chip único de circuito integrado (Integrated Circuit Chip - ICC) poderia ser usado como dispositivo independente (standalone), ou poderia estar embutido/confinado dentro de um produto (material de área delimitada), que está ou não fisicamente protegido. Por exemplo, módulos criptográficos de chip único incluem os cartões inteligentes (Smart Cards);

Negociação de chaves (key agreement): Protocolo que possibilita atribuir uma chave simétrica aos participantes legítimos em função de valores secretos definidos por cada um dos participantes, de forma que nenhum dos participantes possa predeterminar o valor da chave. Neste método, a chave não é transferida, nem mesmo de forma cifrada. Exemplo clássico desta classe de protocolo é o algoritmo Diffie-Hellman;

Número de Identificação Pessoal (Personal Identification Number - PIN): um código alfanumérico ou senha usada para autenticar uma identidade;

Número de Registro: Número sequencial atribuído a cada registro, que serve para identificar unicamente o registro dentro de seu EF [ISO/IEC 7816-4];

Oficial de segurança: uma entidade ou processo que age como tal, realizando funções criptográficas de iniciação ou gerenciamento;

Parâmetros críticos de segurança (PCS): Representam informações sensíveis e relacionadas a segurança, tais como, chaves criptográficas privadas, chaves simétricas de caráter secreto, chaves de sessão e dados de autenticação (senhas e PIN, por exemplo), cuja divulgação ou modificação podem comprometer a segurança de um módulo criptográfico;

PC/SC: especificação para integração de cartões inteligentes (smart cards) em sistemas de computação;

PKCS#11: padrão utilizado como interface para invocar operações criptográficas em hardware e é utilizado para prover suporte aos tokens.

Registro: Cadeia (string) de bytes que pode ser manuseada como um todo pelo cartão inteligente e referenciada por um número de registro ou por um identificador de registro [ISO/IEC 7816-4].

Safesign: software gerenciador responsável pela identificação e manutenção dos certificados disponíveis em um hardware criptográfico (cartão inteligente ou Token USB);

Senha: uma cadeia de caracteres (letras, números e outros símbolos) usada para autenticar uma identidade ou para verificar autorizações de acesso.

Software: Programas e componentes de dados usualmente armazenados em mídias que podem ser apagadas (disco rígido, por exemplo), os quais podem ser dinamicamente escritos e modificados durante a execução.

Token: Nome geral de todos os dispositivos criptográficos, tais como cartões inteligentes (smart cards), dispositivos que possuem senhas e funcionalidades de armazenamento de certificados etc.

Token USB PKI: dispositivo criptográfico portátil integrado com smart card e porta USB. Uma das vantagens deste dispositivo sobre os cartões inteligentes é a portabilidade, bem como suporte a aplicações PKI.

Token USB: Dispositivo criptográfico com conector USB, portátil e de fácil uso.

TSP (Token Service Provider): Camada de hardware abstrata presente no framework ePassNG. Esta camada interfaces comuns de entrada e saída para todos os tipos de dispositivos. O design pode prover uma determinada expansão contra as diferenças de hardware.

Transporte de chaves (key transport): Protocolo que possibilita que uma chave simétrica seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.

Unidade de Dado: O menor conjunto de bits que pode ser referenciado de forma não ambígua [ISO/IEC 7816-4].

Usuário: um indivíduo ou processo que age como tal com o intuito de obter acesso a um módulo criptográfico para executar serviços.

2. Lista de Acrônimos

AES Advanced Encryption Standard	IV Initialization Vector
APDU Application Protocol Data Unit	JCE Java Cryptography Extension
API Application Programming Interface	LCR Lista de Certificados Revogados
ATR Answer To Reset	LEA Laboratório de Ensaios e Auditoria
CBC Cipher Block Chaining	LSITEC Laboratório de Sistemas Integráveis Tecnológico
CE Consumer electronics	MAC Message Authentication Code
CFCA China Financial Certificate Authority	MF Master File
CLK Clock	MSCAPI Microsoft Crypto API
DES Data Encryption Standard	NIST National Institute of Standards and Technology
DF Dedicated File	OPSEC Operations security
EEPROM Electrically Erasable Programmable Read-Only Memory	PC Personal Computer
EF Elementary File	PCS Parâmetros Críticos de Segurança
FCC Federal Communications Commission	PIN Personal Identification Number
FIPS Federal Information Processing Standards	PPS Protocol and Parameters Selection
GND Ground	PUK PIN Unlock Key
ICC Integrated Circuit Chip	RFU Reserved for Future Use
ICP Infraestrutura de Chaves Públicas	RNG Random Number Generator
ICP-Brasil Infraestrutura de Chaves Públicas Brasileira	RSA Rivest Shamir and Adleman
IEC International Electrotechnical Commission	RST Reset
IKE Internet key exchange	SHA Secure Hash Algorithm
IN Instrução Normativa	SO Sistema Operacional
IPSec Internet Protocol Security	SP Service Provider
I/O Input/Output	SSL Secure Sockets Layer
ISO International Organization for Standardization	TLV Tag Length Value
ITL Information Technology Laboratory	TSP Token Service Provider
ITI Instituto Nacional de Tecnologia da Informação	TTL Time To Live
	USB Universal Serial Bus
	VPP Variable Supply Voltage

3. Sobre a Pronova Soluções Inteligentes

A Pronova Soluções Inteligentes é formada por uma equipe com mais de 20 anos de experiência no mercado de Segurança da Informação. Somos pioneiros neste setor, no qual sempre nos destacamos pela qualidade dos produtos que oferecemos aliada ao bom atendimento, formação de parcerias, lançamento de novas tecnologias, além de serviços de consultoria.

Ao longo deste período, lançamos e comercializamos no Brasil produtos desenvolvidos e utilizados em larga escala no mercado internacional. Atendemos as mais variadas necessidades de proteção, como armazenamento e transmissão segura de informações, monitoramento de conteúdo hostil, além de proteção de software contra pirataria, entre outros.

4. Introdução

Neste documento poderão ser encontrados os procedimentos de instalação, configuração e utilização básica da ferramenta SafeSign Standard 3.0.77, possibilitando o uso de certificados digitais armazenados em Tokens e Cartões Inteligentes no ambiente Mac OS X.

5. Pré-requisitos

Para instalar o SafeSign Identity Client observe os seguintes pré-requisitos:

- Ter condições de se autenticar (logar) como usuário administrador no sistema operacional.
- Não deixar nenhum dispositivo criptográfico conectado às portas USB durante a instalação.

6. Ambientes Homologados

A versão 3.0.77 do SafeSign Identity Client foi homologada pela PRONOVA nos seguintes Sistemas Operacionais:

- Mac OS X Snow Leopard (10.6.7)
- Mac OS X Lion (10.7.x)

Navegador Homologado: Mozilla Firefox 16 (ou superior)

Importante: O SafeSign Identity Client 3.0.77 também é compatível com o Mac OS X Mountain Lion (10.8.x). Entretanto, nem todos os sistemas que utilizam certificados digitais padrão ICP-Brasil podem ainda não suportar este sistema. Se desejar, você pode seguir os procedimentos contidos neste manual também para o Mac OS X Mountain Lion (10.8.x), porém, a PRONOVA não se responsabiliza por eventuais falhas na utilização do software até que todos os sistemas que utilizem certificados padrão ICP-Brasil homologuem oficialmente este sistema operacional.

7. Hardwares Homologados

O SafeSign Identity Client 3.0.77 foi homologado pela PRONOVA com os seguintes dispositivos:

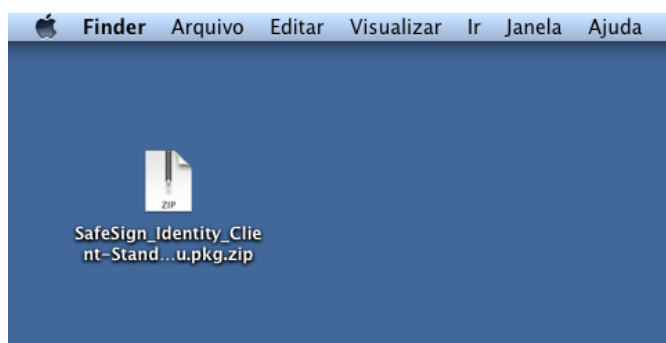
- ProToken Plus Safesign
- StarSign Crypto USB
- Cartão Inteligente Pronova Safesign

8. Instruções de Instalação

A seguir, você encontrará as etapas para instalação do SafeSign 3.0.77.

8.1 Copiar para a Mesa o arquivo de instalação disponível no CD ou Solicitar o Link de Download em http://www.pronova.com.br/contato_safesign.php

A primeira etapa para iniciar a instalação do SafeSign 3.0.77 é ter acesso ao arquivo "SafeSign_Identity_Client-Standard-3.0.77-general-x86_64-macosx-admin-std-gnu.pkg" disponível n CD de instalação ou através de solicitação através do de formulário disponível em http://www.pronova.com.br/contato_safesign.php, é recomendado salvar o arquivo na Mesa (Área de Trabalho do Mac OS X) conforme imagem abaixo:

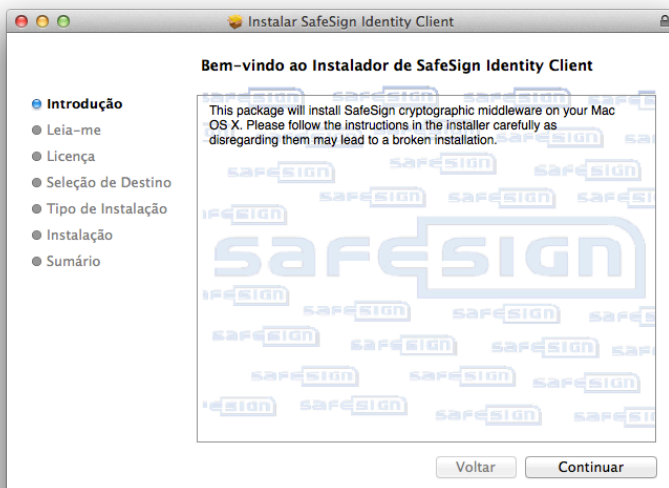


Dê um duplo clique no arquivo " SafeSign_Identity_Client-Standard-3.0.77-general-x86_64-macosx-admin-std-gnu.pkg.zip". Isso fará com que o arquivo seja descompactado, gerando na Mesa (Área de Trabalho) um novo arquivo com o nome "SafeSign_Identity_Client-Standard-3.0.77-general-x86_64-macosx-admin-std-gnu.pkg", conforme imagem abaixo:

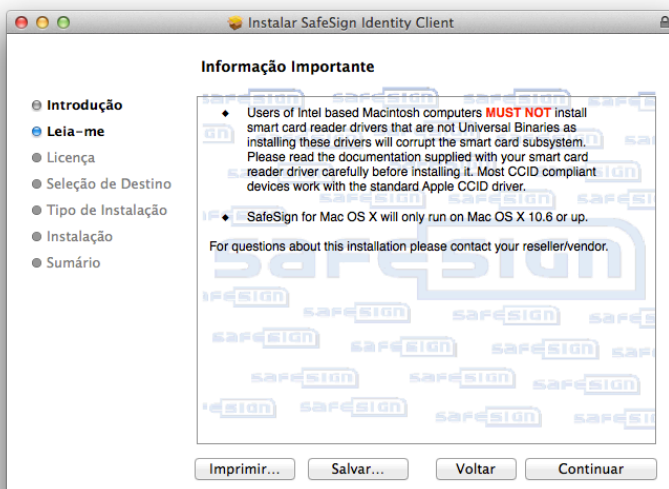


8.2 Como iniciar a instalação?

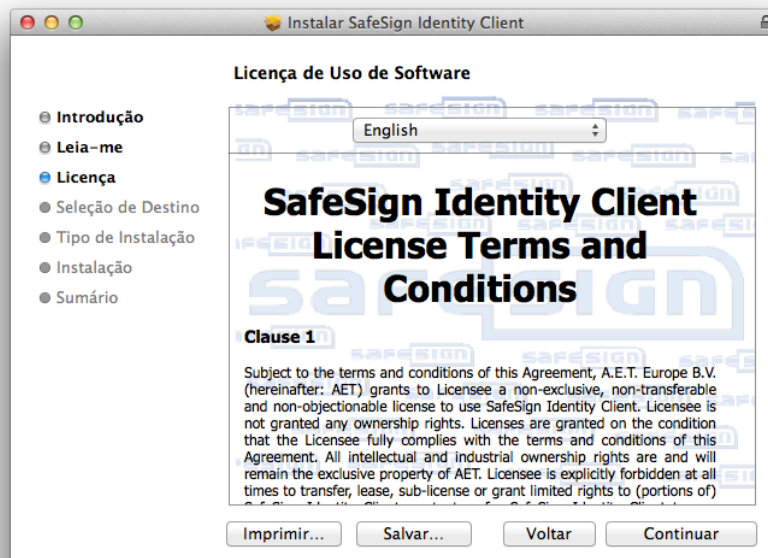
Para prosseguir com a instalação, dê um duplo clique no arquivo "[SafeSign_Identity_Client-Standard-3.0.77-general-x86_64-macosx-admin-std-gnu.pkg](#)", esta ação irá carregar o assistente de instalação do SafeSign conforme a próxima imagem. Clique em "Continuar" para prosseguir com a instalação.



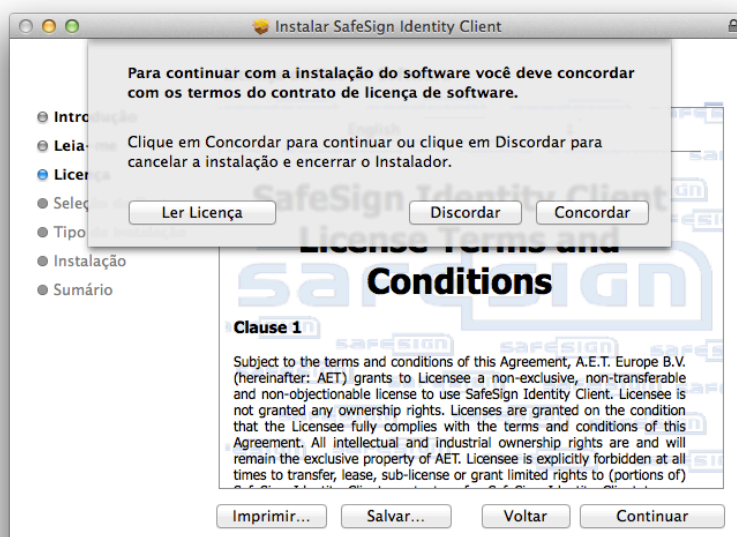
Após clicar em "Continuar", o assistente apresentará um aviso para leitura. Este aviso diz que a instalação de drivers de leitoras podem corromper componentes importantes que atuam no reconhecimento de leitores e tokens. Os leitores homologados pela PRONOVA não necessitam de drivers para Mac OS X, portanto, nenhuma ação especial é necessária neste caso. Clique no botão "Continuar" para dar continuidade à instalação.



Na próxima janela, o assistente apresentará o contrato de licença de uso. Clique no botão “Continuar” para seguir com a instalação.

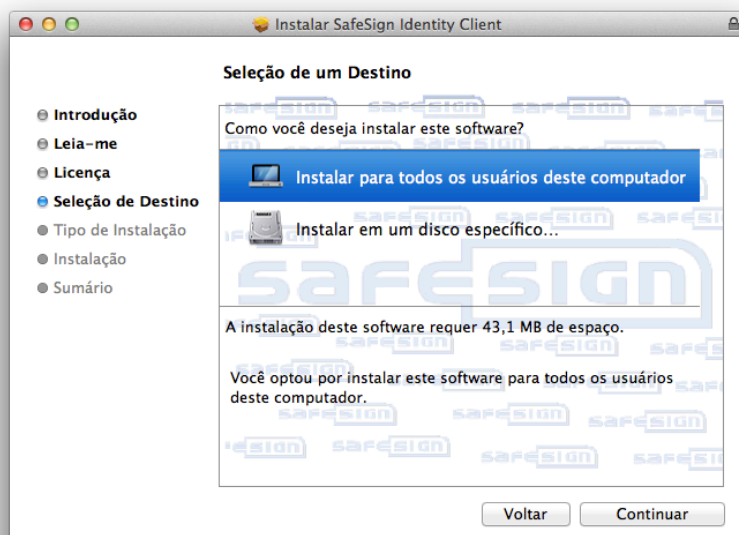


Após clicar em "Continuar", você vai se deparar com uma nova janela perguntando se você concorda ou discorda dos termos de licença, clique em “Concordar”.

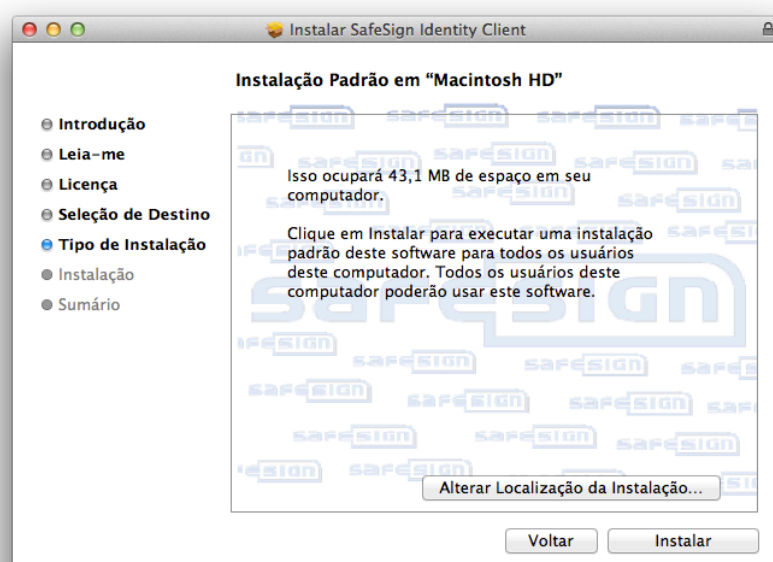


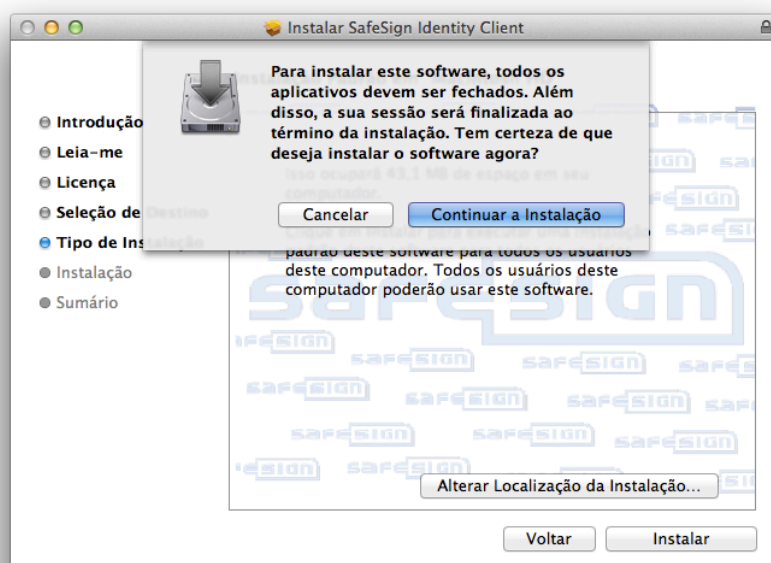
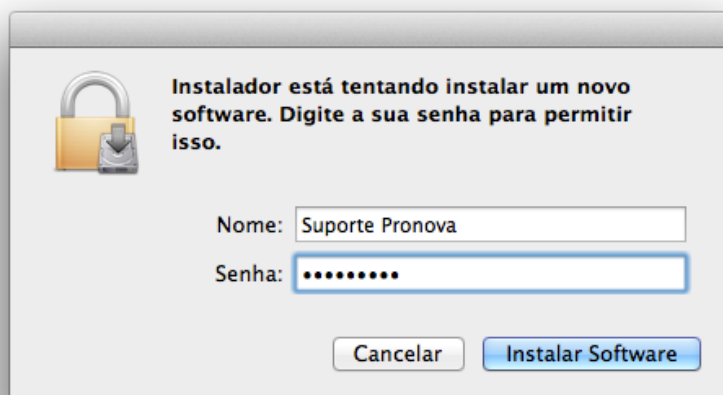
Após aceitar os termos de uso, o assistente selecionará automaticamente o local da

instalação. Para continuar clique em “Instalar para todos os usuários deste computador” e depois clique no botão “Continuar”.

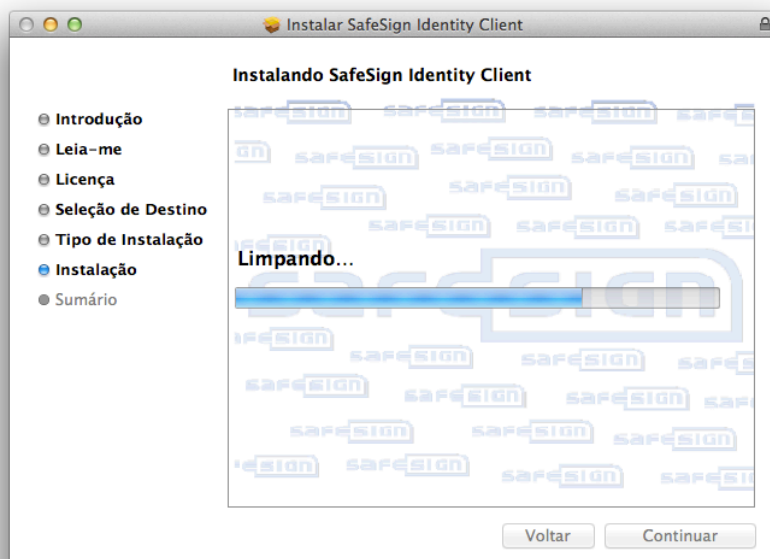


Após clicar no botão "Instalar", o assistente solicitará a sua senha de administrador para poder instalar os arquivos no disco. Digite a sua senha e, posteriormente, clique em “Instalar Software” e em “Continuar a instalação”.

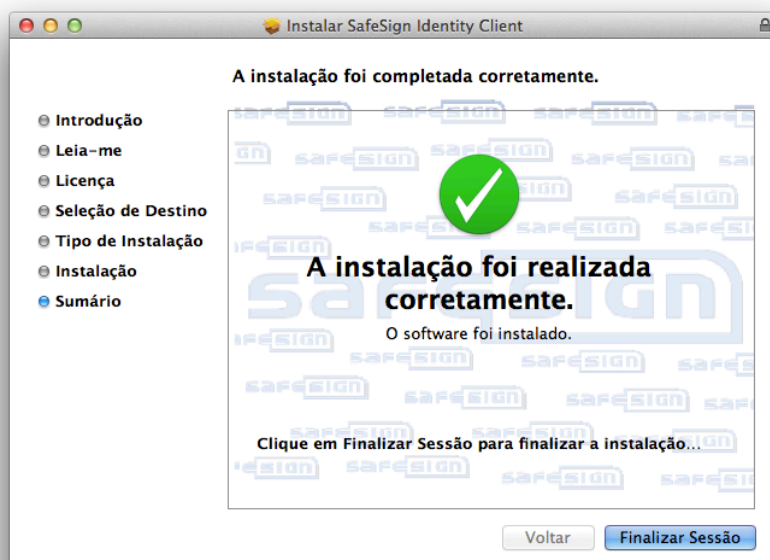




Depois de clicar em “Continuar a Instalação”, ele iniciará o processo de cópia de arquivos. Este processo pode ser acompanhado pela barra de progresso no assistente de instalação, como pode ser observado na próxima imagem.



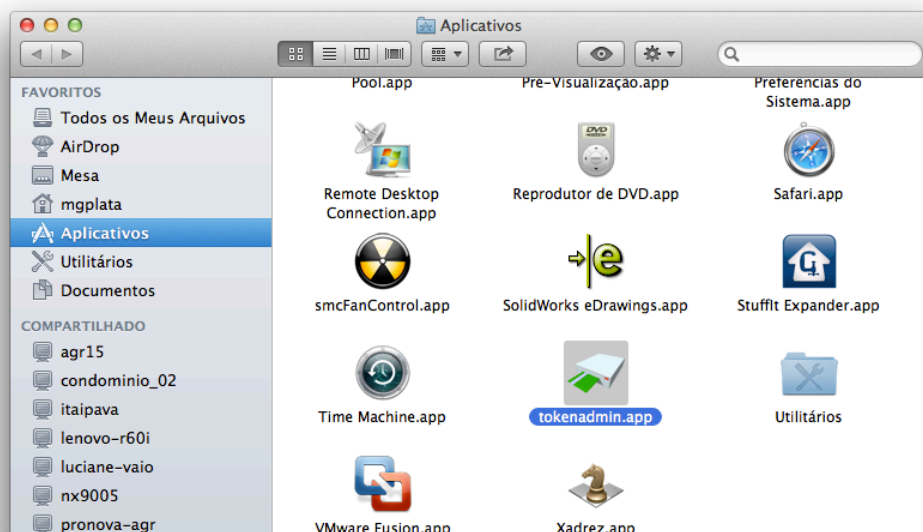
Com o término da cópia dos arquivos, o assistente informará que a instalação foi realizada corretamente. Clique em “Finalizar Sessão” para finalizar o processo de instalação.



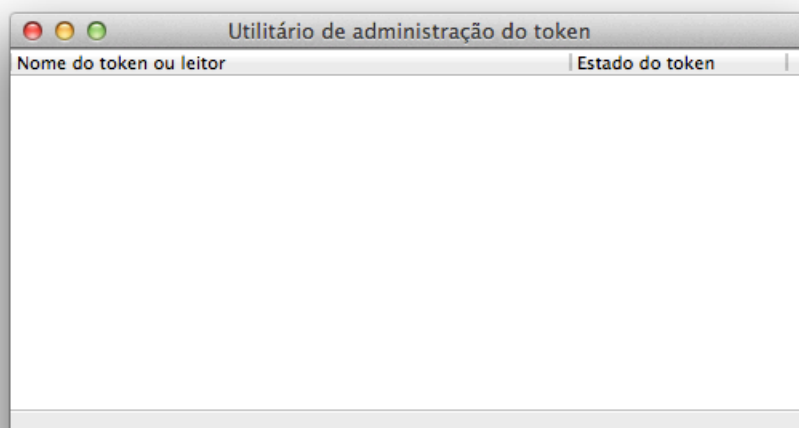
Depois de clicar no botão “Finalizar Sessão”, a sua sessão será encerrada e você terá que se autenticar novamente no seu Mac OS X. Todavia, recomendamos reiniciar o seu Mac !

8.3 – Como verificar a instalação?

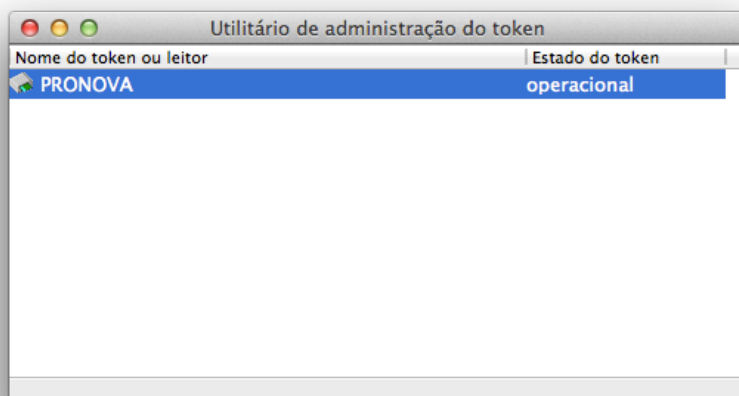
Após a nova autenticação ou reinício do seu Mac, resta saber se o SafeSign foi corretamente instalado. Execute a ferramenta tokenadmin (Utilitário de administração do token). Para iniciar esta ferramenta, é necessário acessar a pasta "Aplicativos" e, posteriormente, clicar duas vezes sobre o ícone "tokenadmin"



Ao clicar duas vezes sobre o ícone "tokenadmin", o Utilitário de administração do token será aberto. Caso a janela abaixo não seja apresentada, entre em contato com o Suporte da Pronova para receber auxílio na instalação do SafeSign:



Através do SafeSign, podemos identificar se o dispositivo está sendo corretamente reconhecido. Para isto, basta conectarmos o dispositivo à porta USB e abrir o SafeSign. Em sua tela inicial, será apresentado o nome do dispositivo (seja leitor/cartão ou Token) e também o status deste dispositivo. No exemplo abaixo, temos um Token conectado e reconhecido corretamente.



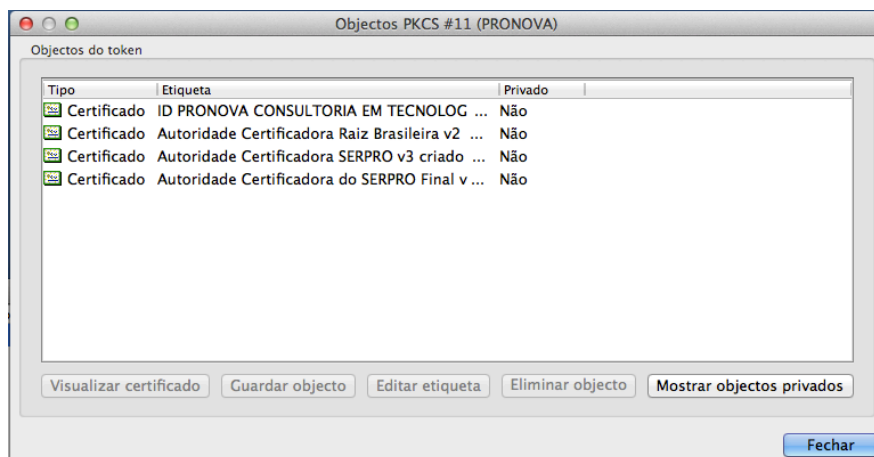
Através deste utilitário podemos saber se a mídia foi devidamente reconhecida a partir do campo status do token, onde é apresentado se o dispositivo está pronto ou não para uso. A seguir, uma tabela com os possíveis status para um dispositivo:

Operacional	indica que o dispositivo foi reconhecido corretamente e está pronto para uso
Presente	indica que uma mídia foi reconhecida, no entanto não está apta para uso
Ausente	indica que um leitor sem cartão inteligente foi reconhecido. Se você utiliza Token, este status não será apresentado
Não Inicializado	indica que o Token ou Cartão foi reconhecido corretamente, no entanto não está pronto para uso, pois existe a possibilidade do dispositivo ainda não ter sido formatado. Em casos assim, é importante entrar em contato com o Suporte da Pronova para receber o auxílio correto

8.4 – Como visualizar o meu certificado?

Agora que temos um dispositivo conectado e devidamente reconhecido como “operacional”, podemos visualizar o conteúdo deste para verificar seus certificados.

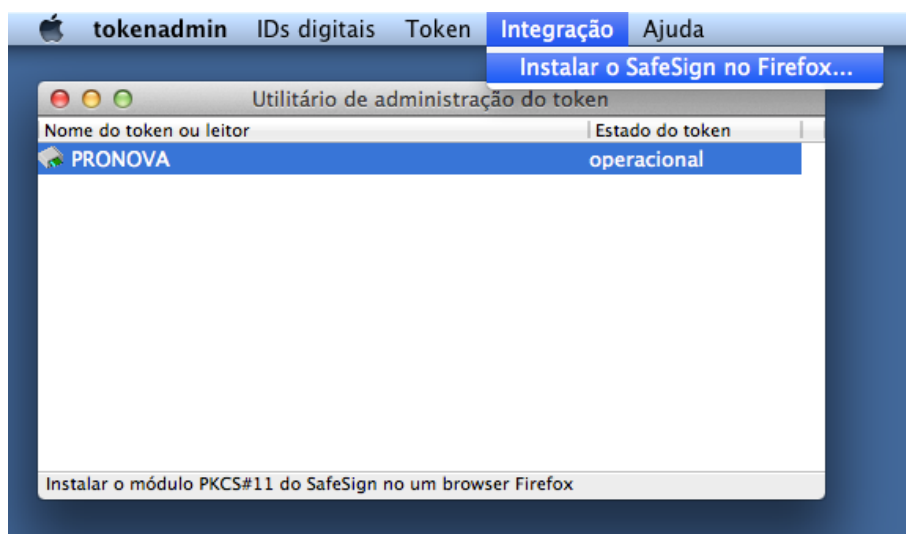
Esta é uma operação muito simples. Basta clicar duas vezes sobre o nome do dispositivo que é apresentado e uma janela será exibida com todo o conteúdo, conforme a próxima imagem.



8.5 – Como testar o meu certificado usando o Mozilla Firefox?

O SafeSign 3.0.77 pode ser utilizado somente no navegador Mozilla Firefox, todavia, para que funcione corretamente, algumas configurações são necessárias. Abaixo, seguem as instruções.

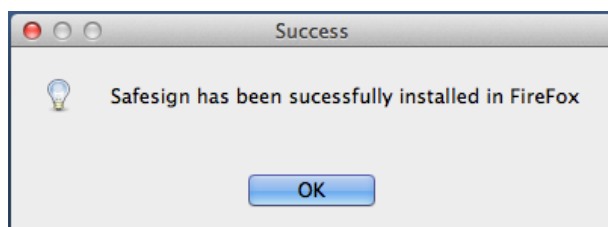
Abrir a ferramenta Utilitário de administração do Token e na barra de menu, clicar em “Integração” e depois em “Instalar o Safesign no Firefox...” conforme a imagem abaixo:



Na próxima janela que será exibida, clique em Firefox e depois no botão “Instalar”



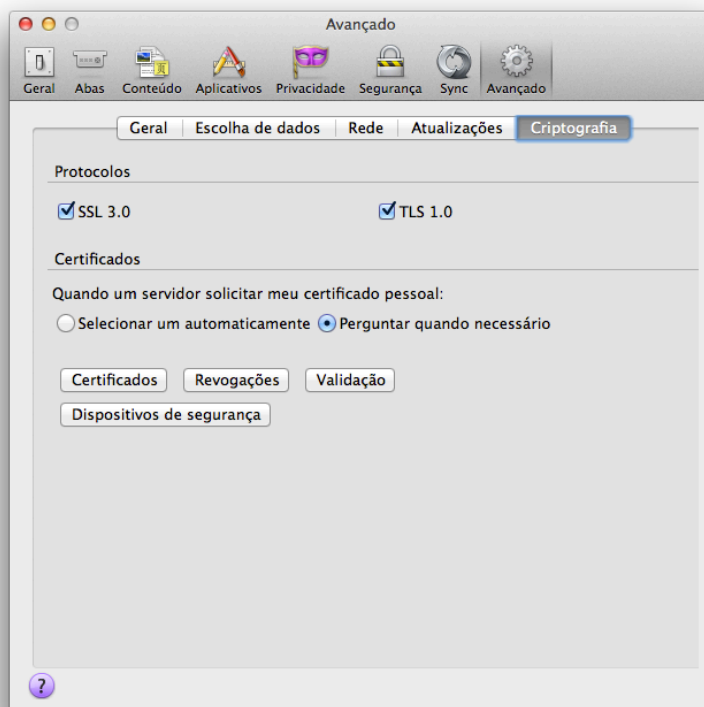
Ao final a mensagem “Safesign has been sucessfully installed in Firefox” será exibida. Clique no botão “OK”, depois no botão “Fechar” da janela anterior e por fim encerrar o Utilitário de administração.



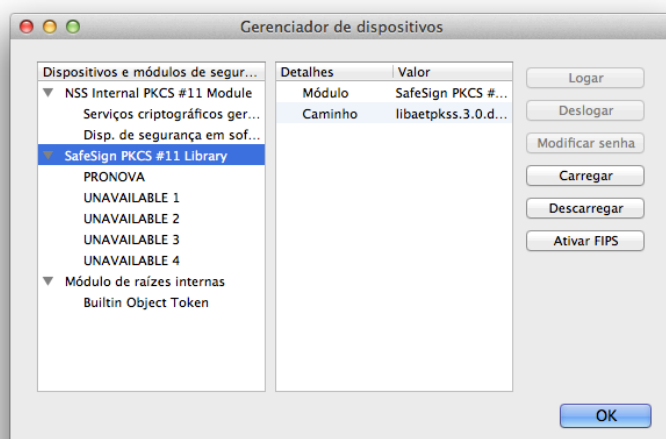
Para confirmar se a integração com o Firefox foi realizada com sucesso, abrir o Mozilla Firefox e, no menu, clique em “Firefox”. Depois, clique sobre a opção “Preferências”, conforme a próxima imagem.



Ao clicar em preferências, uma janela aparecerá com diversas opções disponíveis. Na parte superior desta janela, clique no ícone “Avançado”, depois na aba “Criptografia”, e, dentro “Criptografia” clicar no botão “Dispositivos de segurança”.

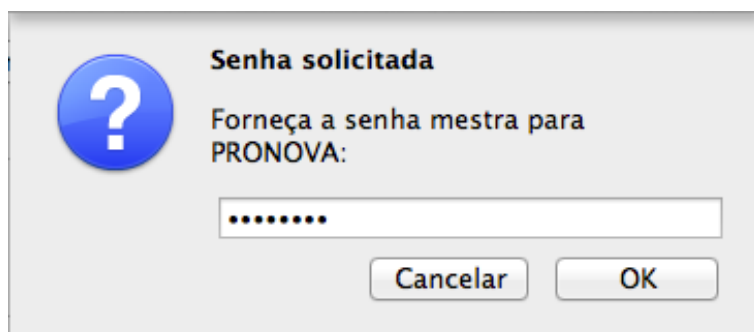


Uma nova janela chamada “Gerenciador de dispositivos” será exibida. É nesta janela que deverá estar presente o modulo Safesign PKCS #11 Library na coluna “Dispositivos e módulos de segurança”.

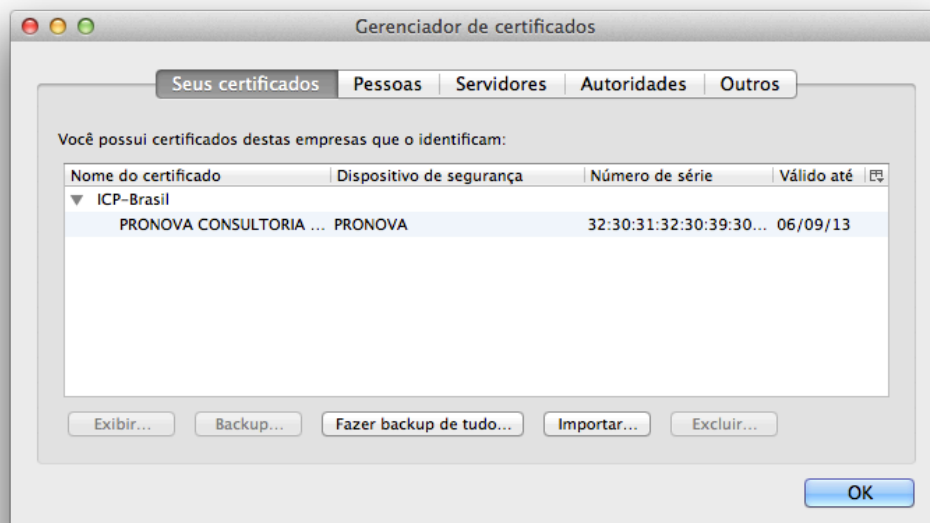


Se este módulo “Safesign PKCS #11 Library” não estiver presente, entre em contato com o Suporte Pronova !

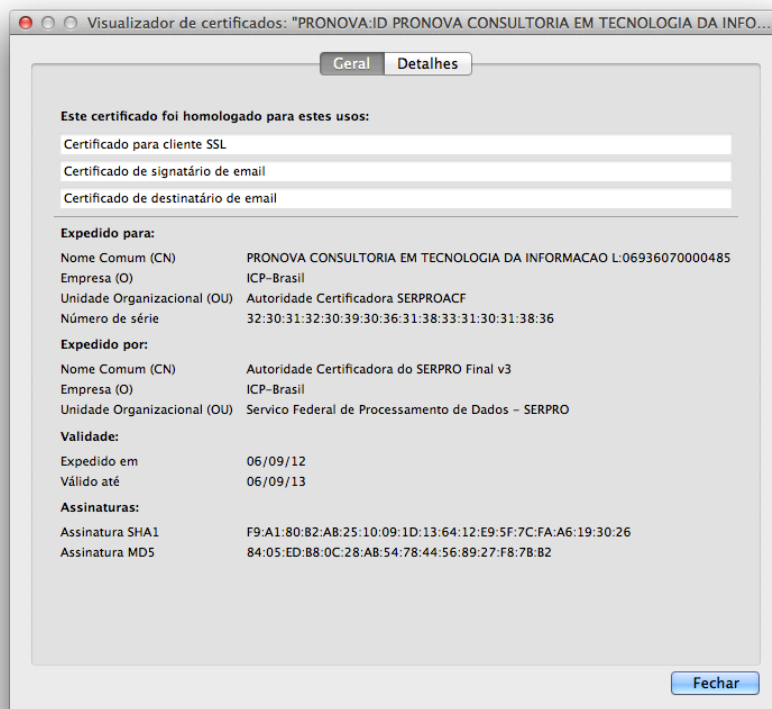
Se o modulo estiver presente, volte para a aba "Criptografia" do menu de configurações avançadas do Mozilla Firefox e clique no botão “Certificados”. Repare que será necessário informar a senha mestra (PIN) de seu dispositivo,. Digite o PIN e clique em “OK”



Se o PIN digitado estiver correto, o Mozilla Firefox abrirá uma nova janela chamada “Gerenciador de Certificados”. Verifique se o certificado gravado dentro do seu dispositivo está presente na aba “Seus Certificados”.



Clicando duas vezes sobre um certificado, uma janela será aberta mostrando todas as informações do mesmo, conforme a imagem na próxima página.

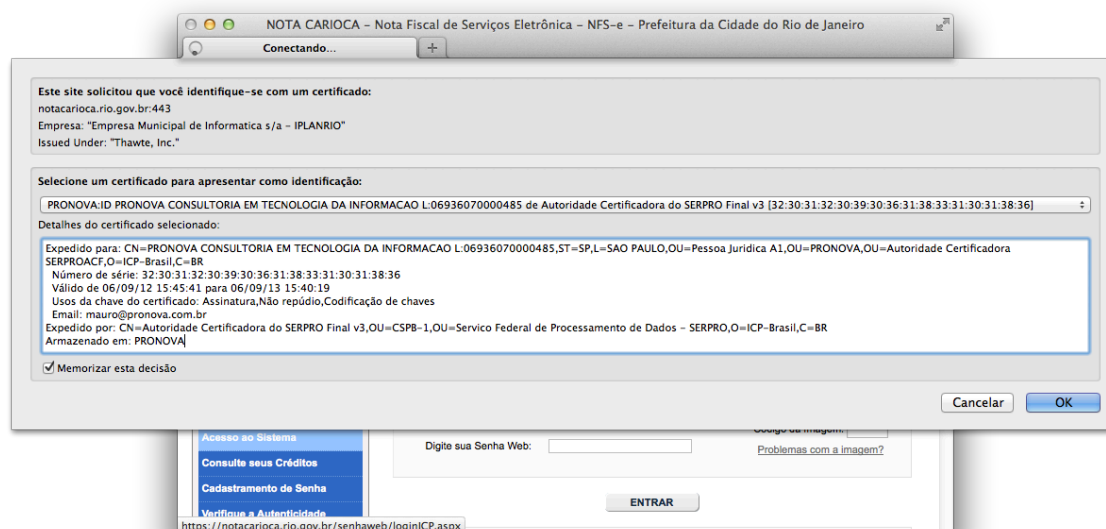


Agora que confirmamos que o módulo está instalado e que o certificado está disponível para o Firefox, você poderá testá-lo no site do e-CAC ou em qualquer outro site que aceite certificados padrão ICP-Brasil. Aqui neste documento, utilizaremos o Site da Nota Fiscal Carioca.



Caso você ainda não fornecido o PIN do seu dispositivo, ao clicar na imagem “Possui Certificado Digital ICP-Brasil” o navegador poderá solicitar a senha mestra (PIN) para acessar seu dispositivo, desta forma, ele poderá identificar os certificados adequados para a autenticação. Digite o PIN e clique em “OK”.

ATENÇÃO: se a senha não foi alterada por você no momento da validação presencial, a senha será “12345678” (sem as aspas). Após digitar o PIN do dispositivo, será apresentada uma lista com os certificados encontrados. Escolha qual certificado deseja realizar a autenticação e clique em “OK”.



Depois de selecionar o certificado, você deve ser redirecionado para a seguinte página onde será possível confirmar a autenticação checando os dados na parte superior da janela do navegador, como ilustrado na imagem da próxima página.



Com isso, o processo estará concluído. Se você seguiu todos os procedimentos conforme descrito neste documento e, mesmo assim, seu certificado não funciona em seu Mac OS X, não deixe de entrar em contato com o Suporte da Pronova para receber auxílio.

NOTA: além da instalação do módulo PKCS#11, também é necessário fazer a instalação da cadeia de certificados da Autoridade Certificadora que emitiu o certificado que está gravado no seu Dispositivo Safesign. Se a instalação da cadeia não for realizada, embora a instalação do módulo tenha sido realizada com sucesso o certificado não será reconhecido como válido pelo navegador e não poderá ser usado nos serviços que demandam certificados ICP-Brasil. Assim, mantenha contato com o Suporte Técnico da Autoridade que emitiu o seu certificado e solicite as instruções para fazer a instalação da cadeia de certificados.

9. Perguntas e Respostas

1) Fiz meu certificado A3 com a Pronova e agora quero usar o Token no meu computador. Preciso executar algum procedimento de inicialização do Token onde está gravado o meu certificado?

R: Não! Para o software Safesign a função INICIALIZAR ou APAGAR tem o mesmo efeito de FORMATAR. Assim sendo, se o seu Token já possui um certificado gravado, não inicialize ou apague o seu Token !

2) Comprei novos dispositivos Safesign, preciso reinstalar o Safesign Standard?

R: Se sua máquina estiver com a versão 3.0.45 ou superior não é necessário fazer uma nova instalação. Todavia, se a versão do Safesign instalada em sua máquina for inferior a versão 3.0.45, você deverá remover a versão ora instalada, depois reiniciar o computador e somente depois deste novo boot fazer a nova instalação usando o instalador disponível no CD de instalação ou através do link de download fornecido pelo Suporte da Pronova.

10. Suporte Técnico

Se as informações contidas neste guia rápido não foram suficientes, não se preocupe, durante o período de garantia de 90 (noventa) dias entre em contato conosco sempre que precisar. O telefone para contato é (21) 2491-3688 ou (24) 2222-2230.